EXHIBIT A

Requirements for the Protection of
Unencrypted Digital Terrestrial Broadcast Content
Against Unauthorized Redistribution

Joint Proposal from MPAA and 5C Companies
December 6, 2002

[Excerpted January 2, 2004]

Scope

. . .

[X.] Requirements.

X.1 Definitions.

. . .

"Circumvention Devices" means devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies used to meet the requirements set forth in this Section X.

. . .

"Demodulator Robustness Requirements" means the requirements set out in Sections X.7 through X.12.

. . .

"Hardware" means a physical device, including a component, that implements in a Covered Demodulator Product . . . any of the content protection requirements set forth in the respective Demodulator Compliance Requirements . . . and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such product or (ii) includes instructions or data that are not permanently embedded in such product where such instructions or data have been customized for such product and such instructions or data are not accessible to the end user through the product.

. . .

"Robust Method" means, with respect to the passing of Unscreened Content or Marked Content from one product to another, a method that complies with Section X.10.

"Software" means the implementation in a Covered Demodulator Product . . . of any of the content protection requirements set forth in the respective Demodulator Compliance Requirements . . . through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware.

. . .

X.7 Robustness Requirements for Covered Demodulator Products: Construction.

(a) Covered Demodulator Products shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such products to defeat the Demodulator Compliance Requirements.

(b) Covered Demodulator Products shall not include:

(1) switches, buttons, jumpers or software equivalents thereof,

(2) specific traces that can be cut, or

(3) functions (including service menus and remote-control functions),

in each case by which the Demodulator Compliance Requirements can be defeated, or by which compressed unencrypted Marked Content or compressed unencrypted Unscreened Content in such Covered Demodulator Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Section X.[1,2]

(c) Covered Demodulator Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal any secret keys or secret algorithms used to meet the requirements set forth in the Demodulator Compliance Requirements.

X.8 Robustness Requirements for Covered Demodulator Products: Data Paths. Within a Covered Demodulator Product, neither Unscreened Content nor Marked Content shall be present on any User Accessible Bus in unencrypted, compressed form.

---

[1] See Section X.8(a). It is anticipated that if the Demodulator Robustness Requirements are modified in the future to require protection of uncompressed data on a User Accessible Bus, the requirements of Section X.7(b) would also then be modified to apply to uncompressed unencrypted content.

[2] For avoidance of doubt, the provisions of Section X.7(b) prohibit inclusion of such means by which such defeating or exposure can occur through removal of the Broadcast Flag.

(a) Uncompressed Content. During a petition opportunity that the Commission may designate, an interested person may petition the Commission to initiate a Notice of Inquiry to determine whether it is technically feasible and commercially reasonable to require that Unscreened Content and Marked Content when transmitted over any User Accessible Bus in uncompressed digital form be made reasonably secure from unauthorized interception by using means that meet the standards set forth in Section X.11. Such petition shall include evidence that such an inquiry is warranted in light of generally available technologies and existing commercial circumstances. Should the Commission, based on such evidence and on consultation with affected industries, proceed with such Notice of Inquiry and thereby determine that requiring such protection at such level is technically feasible and commercially reasonable, the Commission may, pursuant to a Notice of Proposed Rulemaking, revise these Demodulator Robustness Requirements to so require. The Commission will consider in its analysis: the general availability of relevant technologies, cost of implementation, effectiveness of any solutions, availability of alternative solutions, intellectual property licensing issues, consistency with requirements of other content protection systems, likely ability of manufacturers of Covered Demodulator Products to satisfy the Demodulator Robustness Requirements, and normal design cycles for such products. The Commission will exercise its discretion to limit the frequency of such Notices of Proposed Rulemaking.

X.9 Methods of Making Functions in Covered Demodulator Products Robust. Covered Demodulator Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

(a) Distributed Functions. Where compressed Unscreened Content or compressed Marked Content is delivered from one portion of the Covered Demodulator Product to another portion of such Covered Demodulator Product, whether among integrated circuits, software modules, a combination thereof, or otherwise, such portions shall be designed and manufactured in a manner associated and otherwise integrated with each other such that such Unscreened Content or Marked Content, as the case may be, in any usable form flowing between such portions of such Covered Demodulator Product shall be reasonably secure from being intercepted or copied except as permitted under the Demodulator Compliance Requirements.

(b) Software. Without limiting the requirements of Sections X.7 and X.8, portions of a Covered Demodulator Product that implement in Software the content protection requirements set forth in the Demodulator Compliance Requirements shall:

(1) Comply with Section X.7(c) by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode (i.e. in kernel mode), and/or embodiment in a secure physical

implementation; and, in addition, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

(2) Be designed so as to perform or ensure checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide access to unencrypted Unscreened Content or unencrypted Marked Content. For purposes of this Section X.9(b)(2), a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections X.7 and X.8. This Section X.9(b)(2) requires at a minimum the use of signed code or more robust means of "tagging" operating throughout the code. For purposes of this Section X.9(b), "signed code" means a method of achieving trusted distribution of Software by using public key cryptography, keyed hash, or other means at least as effective, to form a digital signature over Software such that its authenticity and integrity can be verified.

(c) Hardware. Without limiting the requirements of Sections X.7 and X.8, the portions of a Covered Demodulator Product that implement in Hardware the content protection requirements set forth in the Demodulator Compliance Requirements shall:

(1) Comply with Section X.7(c) by any reasonable method including but not limited to (x) embedding any secret keys or secret cryptographic algorithms used to meet the content protection requirements set forth in the Demodulator Compliance Requirements in silicon circuitry or firmware that cannot reasonably be read or (y) employing the techniques described above for Software.

(2) Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements set forth in the Demodulator Compliance Requirements in Covered Demodulator Products would pose a serious risk of rendering the Covered Demodulator Product unable to receive, demodulate, or decode Unencrypted Digital Terrestrial Broadcast Content. By way of example, a component that is soldered rather than socketed, or affixed with epoxy, may be appropriate for this means.

(d) Hybrid. The interfaces between Hardware and Software portions of a Covered Demodulator Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection that would be provided by a pure Software implementation.

X.10 Robustness Requirements for Covered Demodulator Products: Robust Methods. Where a Covered Demodulator Product passes, or directs to be passed, Unscreened Content or Marked Content from such Covered Demodulator Product to

another product pursuant to Section X.6(a), it shall do so using a method designed to ensure that such content, in any usable form, shall be reasonably secure from being intercepted, redistributed or copied when being so passed to such other product. Where a Covered Demodulator Product passes, or directs to be passed, Unscreened Content to an output pursuant to Section X.3(a)(4), it shall do so using a method that provides technological protection against unauthorized redistribution of such content that is at least as effective as such technological protection provided by any one of the Authorized Digital Output Protection Technologies and that is designed to ensure that such content may be accessed in usable form by another product only if such other product is a Downstream Product.

X.11 Robustness Requirements for Covered Demodulator Products: Level of Protection. The content protection requirements set forth in the Demodulator Compliance Requirements and the requirements set forth in Sections X.7(c) and X.8 shall be implemented in a reasonable method so that they:

(a) Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons, or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers, other than Circumvention Devices; and

(b) Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section X.11(a) such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

X.12 Robustness Requirements for Covered Demodulator Products: Advance of Technology. Although an implementation of a Covered Demodulator Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Covered Demodulator Product, would have caused such products to fail to comply with these Demodulator Robustness Requirements ("New Circumstances"). If a manufacturer of a Covered Demodulator Product has actual notice or actual knowledge of New Circumstances that relate to the manufacturer's specific implementation of a Covered Demodulator Product (hereinafter referred to as "Notice"), then within 18 months after Notice such manufacturer shall cease distribution of such Covered Demodulator Product and shall only distribute Covered Demodulator Products that are compliant with the Demodulator Robustness Requirements in view of the then-current circumstances.

. . .